PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/20 — A2

(11) International Publication Number: **WO 98/56192**

(43) International Publication Date: 10 December 1998 (10.12.98)

(21) International Application Number: PCT/IL98/00253

(22) International Filing Date: 1 June 1998 (01.06.98)

(30) Priority Data:

60/048,243	2 June 1997 (02.06.97)	US
08/977,605	25 November 1997 (25.11.97)	US

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

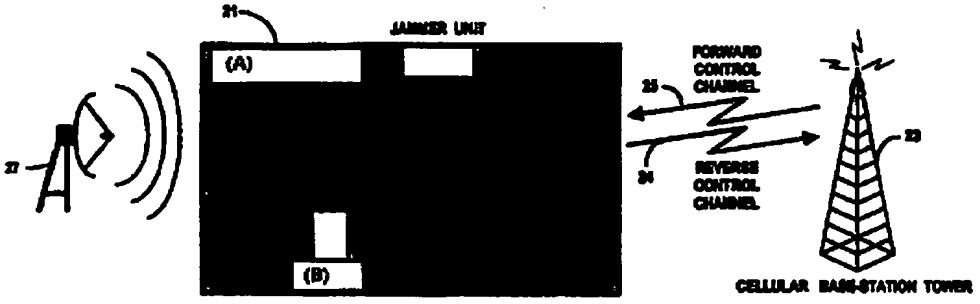
(71) Applicant *(for all designated States except US)*: NETLINE COMMUNICATIONS TECHNOLOGIES (NCT) LTD. [IL/IL]; Hayarden Street 62, 52333 Ramat-Gan (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: ISRAELI, Gil [IL/IL]; Hagefen Street 38, 99797 Karme-Yosef (IL). TE-ENI, Ben, G. [IL/IL]; Ir-Shemesh Street 53A, 69086 Tel-Aviv (IL). YARDEN-ZASLAVSKY, Ofer [IL/IL]; 42855 Moshav Olesh (IL).

(74) Common Representative: ISRAELI, Gil; Hayarden Street 62, 52333 Ramat-Gan (IL).

(54) Title: CELLULAR COMMUNICATIONS FIREWALL



(A)—REGULATED AREA
(B)—MOBILE UNIT

(57) Abstract

A method and system for controlling the use of mobile cellular communications within defined regulated areas are disclosed. The system transmits RF interfering signals on the frequency band typically used by cellular base stations to prevent effective communications between mobile units located within a given regulated area and cellular base stations. In the preferred embodiment, the system waits until mobile unit transmission from within the regulated area is detected and thereupon transmits a blocking signal which prevents effective handshake from taking place.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

CELLULAR COMMUNICATIONS FIREWALL

FIELD OF THE INVENTION

The present invention relates to a method and system for regulation of mobile cellular telephones usage within defined areas, such as conference rooms, concert halls, cinemas etc.

BACKGROUND OF THE INVENTION

As more subscribers use mobile cellular phones and carry them everywhere, even in places such as concert halls, cinemas, synagogues, churches etc., there is a need for a system that will prevent such mobile phones from ringing and disturbing other people nearby (see S. Teitelbaum "**Cellular Obsession**", Wired Magazine, Wired Ventures Inc. , vol. 5, No. 1, Jan 97, pp. 144-149, 194-196).

Certain cellular telephones incorporate features that minimize the nuisance and yet enable subscribers to notice that a call is being received. One method involves the use of a vibrating mechanism, which replaces the noisy ring (see U.S. Pat. No. 5,404,391). When in vibrating mode, once a call is received, the subscriber feels the vibration of the cellular phone and thus may leave the place and talk without disturbing everybody. The main problem is that only a small percentage of the cellular phones on the market include such a vibrating feature and that even user's who own cellular phones that include this feature may forget, or intentionally refrain from, switching the telephone into vibrating mode.

Furthermore, use of cellular telephones may cause more than acoustic nuisance. According to recent medical research, use of cellular telephones may interfere with the normal operation of heart pacemakers and other medical equipment (see Journal of Medical Engineering & Technology, "**Interference to medical equipment from mobile phones**" 21(3-4):141-6, 1997 May-Aug). Similarly, enforcement of cellular telephone usage policy may be advantageous in proximity to avionic equipment (see U.S. Pat. No. 5,670,742), and other RFI susceptible equipment.

In addition, certain authorities may be interested in preventing cellular subscribers from initiating calls. Such may be the case in military bases where prevention of cellular phone usage is necessary due to security considerations. Currently, various security authorities have recognized an operational need to prevent accidental initiation of calls in maximum security zones so as to prevent accidental transmission of sensitive information over such an insecure channel, regularly monitored by foreign intelligence agencies.

In a typical cellular telephone network each cell site has a base station with a computerized transceiver and an antenna. This radio equipment provides coverage for an area that is usually from two to ten miles in radius. Even smaller cell sites cover tunnels, subways and specific roadways. The amount of area depends on topography, population, and traffic. The mobile telecommunication switching office (MTSO) decides which cell and which frequencies in that cell will be used.

The subscribers communicate with the system when they are within the coverage area of the base stations located in the radio cells. In a typical cellular telephone system, a subscriber station, such as a mobile phone, located in a radio cell tunes the receiver unit of its radio to a signaling channel of a base station located in the radio cell. A signaling channel is used for exchanging messages between the mobile phone and the cellular network, including messages concerning establishment of a connection between a subscriber station and a base station. On the basis of connection establishment, the system controller of the cellular radio network assigns the subscriber stations to actual traffic channels, in which the actual transfer of information, i.e. speech or data, takes place.

Various cellular systems are used worldwide, and communications are carried out in accordance with industry established air interface standards. Following are some standards commonly used in various territories throughout the world and well known to those skilled in the art:

(a) AMPS (Advanced Mobile Phone Service) – an analog system based on FDMA (Frequency Division Multiple Access) as defined in EIA/TIA 533 standard;

A further object is to provide a method for preventing cellular telephone calls within defined areas without transmitting a continuos signal.

A further object is to provide a method for preventing cellular telephone calls within defined areas without interfering with normal cellular communication outside said hall.

Yet another object of the present invention is to provide a method for enabling certain high priority subscribers to receive, initiate and conduct calls when located within the hall, despite the blocking of all other subscribers.

Further objects of the invention will become apparent from the description of the invention which follows.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an illustrative diagram describing a typical cellular system composed of 7 cell sites, each having a base station incorporating a transceiver.

FIG. 2 is a functional block diagram of a typical regulated area within the cellular system coverage area, controlled by the present invention.

FIG. 3 is an electronic block diagram of a basic jamming device in accordance with the present invention.

FIG. 4 is a schematic block diagram of an improved embodiment of the present invention where jamming is triggered by mobile unit transmission.

FIG. 5 is a block diagram of an electronic device for scanning a plurality of control channels so as to determine the received signal strength of each channel.

FIG. 6 is a block diagram of a frequency hopping spread spectrum transmitter.

For example, U.S. Pat. No. 5,670,742 was issued on Sep. 23, 1997 to Jones, Scott A for "EMI PROTECTED AIRCRAFT". This device relates to shielding for an aircraft, which protects the aircraft's avionics and other electronic equipment from electromagnetic interference generated by electronic devices in use aboard the aircraft. Such shielding protects from electromagnetic interference (EMI) which might affect an aircraft's avionics and other electronic equipment with potentially disastrous results if the interference occurs at an inopportune time during a flight, such as take-off or landing. This device requires physical modifications to an aircraft, and therefore involves an expensive and time consuming upgrade for each aircraft. Employing similar techniques for other applications may be inefficient and costly.

Radio jamming is a method commonly used for military electronic warfare. Basic jamming devices generate and transmit spot or barrage noise. When applied on the target receiver(s), such jamming signals may significantly reduce the S/N ratio, thereby interfering the communications on the target radio link. Jamming devices consist essentially of a noise source, a modulator and a transmitter. A basic jamming device is disclosed in U.S. Patent No. 3,942,179 issued on Mar. 2, 1976 to Dorn for "FILTERED-NOISE JAMMER". Jammers used for military purposes normally employ powerful transmitters for the purpose of impairing message transmission by the enemy over as large an operation range as possible. Use of plain broadband noise jamming may have several disadvantages, as follows:
(a) high transmission power; (b) difficulty to precisely control a predefined jamming area; (c) interference with low powered signals from remote cell sites.

SUMMARY OF INVENTION

According to one broad aspect of the present invention, a cellular telephony usage control system comprises at least one jammer unit that controls the use of cellular telephones within a geographical area covered by at least one cellular communications system. Continuous transmission of a jamming signal on all control frequencies may be result in inaccurate coverage of jamming, and may negatively effect the performance of the cellular system.

Accordingly, it is a principal object of the present invention to provide a method and device for achieving reliable and accurate prevention of cellular telephone calls, within a given area.

In accordance with a preferred embodiment of the present invention, there is provided a method for prevention of cellular telephone calls in a communication system within a given area, said method comprising the steps of: determining at least one control channel frequency existing within the area for establishing cellular telephone calls, said control frequency containing information transmitted thereon, said information being transmitted as coded signals and commands; and generating a signal which interferes with said control frequency by preventing decoding of said signals and commands, said signal preventing generation of handshake signals in the system, to prevent establishment of a cellular phone call. In the preferred embodiment, the device and method operate to block the control frequencies of the cellular system within a given area. The device transmits a blocking signal with a low power output, which interferes with the ability to receive and decode signals and commands broadcast at the control frequency. Thus, the handshake routine of the mobile with a local cellular base station is prevented. Operation of the device is achieved in several ways, manually, automatically, and/or by remote control. Its operation prevents cellular communication ability by subscribers within the area or within the effective blocking range, which is derived from the effective radiated power (ERP) of the blocking signal, its type and the type of communications/ or blocked system. Using the inventive device, a given area normally accessible by cellular communications is blocked from such access, thus providing a security-related, cultural or other safeguard. The given area is thereby isolated from cellular communications, and access can only be achieved by physically relocating the user whose cellular telephone has been blocked. Other features and advantages of the invention will become apparent from the following drawings and description.

OBJECTS AND ADVANTAGES

Accordingly it is an object of the invention to provide a method for preventing a cellular phone from being able to receive calls when located within a hall, by transmitting a low power RF signal.

FIG. 7 illustrates a jamming system having a sensor device located outside the regulated area to improve accuracy.

FIG. 8 illustrates a non-continuously transmitting jamming device.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates a basic cellular system having 7 hexagonal cells numbered 1-7. Cell 7 is shown in the center, surrounded by adjacent cells 1-6. The serving area of a mobile telephone system would typically contain more than 7 cells, however, for ease of reference, only 7 cells are shown in FIG. 1. Each cell 1-7 contains a base station including a transmitter, receiver and base station controller as are well known in the art. The base station transmitter/receiver is connected to an antenna tower 11-17 which is used to transmit signals to, and receive signals from, mobile telephones, within the mobile telephone system serving area. In FIG. 1 the base stations antenna towers 11-17 are selected to be located at the center of each of the cells 1-7, respectively and are equipped with Omni-directional antennas. However, in other configurations of a cellular radio system, the base station towers 11-17 may be located near the periphery, or otherwise away from the center of the cells 1-7 and may illuminate the cells 1-7 with radio signals either Omni-directionally or directionally. Therefore, the representation of the cellular radio system of FIG. 1 is for purposes of illustration only and is not intended as a limitation on the possible implementations of a mobile radio communications system within which a regulated area is defined for the purpose of controlling use of cellular phones therein. A regulated area 10 is located within cell 7, and a plurality of mobile units are used across the entire serving area within cells 1-7. Again, only one regulated area is shown in FIG. 1, but it should be understood that the actual number of regulated areas can be larger, in practice.

Each cell 1-7 has assigned to it a plurality of voice or speech channels for transmitting and receiving voice signals, and at least one access or control channel for transmitting control data signals, such as a forward control channel, and receiving control data signals from the mobile units, such as a reverse control channel.

(b) D-AMPS (Digital AMPS) – a digital system based on TDMA (Time Division Multiple Access) as defined in IS-54 and IS-136 standards;

(c) GSM (Global System for Mobiles) – a digital system based on TDMA as defined by the European Telecommunications Standards Institute (ETSI) technical specifications;

(d) CDMA (Code Division Multiple Access) – a digital system based on spread spectrum radio communications as defined in IS-95 standard.

The above methods for cellular communications and further systems vary in frequency range, modulation, signal processing, data compression, bandwidth allocation, number of channels and other characteristics.

In a typical cellular system, mobile units communicate with cellular base stations by using two types of channels: control/access channels and voice/data channels. Control channels transfer signaling messages between the base stations and the mobile units, so as to enable paging, call establishment/termination and traffic management. Voice channels carry the actual conversation between the cellular subscriber and the other end of the call.

Since cellular systems rely on wireless communication links, it is required that both control and voice channels maintain a sufficient signal-to-noise (S/N) ratio to enable a reasonable quality of service. In the event that the control channel S/N ratio falls below a minimum level, the mobile unit cannot communicate with the base station and therefore scans other control channels to remain in contact with the cellular system. If no other control channel with a sufficient S/N ratio is detected, the mobile unit cannot contact or be contacted by the cellular system and indicates *No Service*.

There are two main methods for significantly decreasing the S/N ratio of a wireless RF link: physical isolation and jamming.

The first method involves a contiguous conductive shield, well known as a "Faraday cage", which blocks electromagnetic radiation by reflecting, absorbing and dissipating radio frequency signals.

As is known in the art, a cellular phone call can be established either by a subscriber who initiates a conversation (origination), or by a subscriber who receives a conversation (page). In each case, a control channel is used to begin a handshake routine opposite the local cellular base station, which provides service in a given area. A channel can be defined as a specific frequency (as in AMPS), frequency and time-slot (as in TDMA) or a spreading code channel (as in CDMA). Typically, after the handshake process is completed over the control channel, the cellular system allocates a voice channel wherein a further testing is made before the actual conversation begins. Once both forward (base station transmit) and reverse (mobile unit transmit) control channels have been tested, the call is commenced.

Referring to FIG. 2, a regulated area 21 containing at least one cellular mobile unit 22, which communicates with a nearby cellular base station 23. Any communication is initiated over the control channel, in which the base station 23 transmits on the forward control channel 24 and the mobile unit 22 transmits on the reverse control channel 25. A jammer unit 26 is typically located within the regulated area 21 so as to take advantage of the –10 dB (approx.) isolation normally provided by walls surrounding the regulated area. The jammer unit typically transmits a uniform density noise signal at the forward control channel frequency range. It should be understood that various types of noise signals may be used and the exact implementation shall vary according to the cellular standard modulation technique. Preferably, the noise signal level is sufficiently high to raise the noise floor and to capture the demodulator of the mobile units located within the regulated area. However, the noise signal may propagate outside the regulated area and cause interference with cellular subscribers for whom the regulation should not apply. Therefore, the exact level of noise transmitted within the regulated area is a tradeoff involving the forward control channel RF level received within the regulated area, and the isolation provided by the of the regulated area. In various implementations, a jammer unit 27 can be located outside the regulated area 21 whereby using a directional antenna the interfering signal propagation is directed into the regulated area.

Referring now to FIG. 3, there is shown a block diagram of an electronic jammer device for preventing cellular phone calls in a given regulated area. Jammer device provides a shaped signal in the spectral frequency range of the relevant control signal

frequencies of the cellular system. The blocking signal matches the range of control frequencies, and the chosen method of blocking system operation. Jammer device comprises a low-power signal oscillator 30, for generating a blocking signal, and a high-power RF module 35 for transmitting the blocking signal on the RF frequencies desired, via an antenna 33, which is matched to the proper frequency range. A controller 32 controls the modules described above, provides indicator signals and receives remote commands. Specifically, controller 32 controls the operation of the signal oscillator 30 and the transmitter 35, respectively, via control signals 321-322. Controller 32 receives external handshake signals 323 and provides indicator signals 323 for external use. A power supply 34 supplies circuit power. Signal oscillator 30 comprises a modulator 302, a voltage controlled oscillator (VCO) 303, a signal frequency comb oscillator 301 or noise oscillator, a switch 304, a mixer 306, a local oscillator 305, a bandpass filter 307 and an output amplifier 308. As stated above, the chosen method of blocking the cellular system operation determines the operation of jamming device. For example, if a continuous blocking signal on a single control frequency is chosen, modulator 302 is inoperative and VCO 303 generates a coherent signal (within the VCO limitations), which matches the bandwidth of a single control frequency. This signal is forwarded via switch 304 to mixer 306, where it is multiplied by the local oscillator in multiplier 305, to raise it to the required frequency. Signal filter 307 removes unwanted frequencies from the mixer 306 output, and a signal at the chosen blocking frequency is received. Output amplifier 308 amplifies the blocking signal before it is fed to transmitter 35. The blocking signal interferes with the control frequency, to prevent cellular calls. Another method of blocking cellular system operation is to operate jamming device such that a modulated noise signal is produced. In this approach, modulator 302 operates to feed VCO 303 which produces a modulated noise signal.

There are two types of noise signals available in this approach: 1) Analog noise - modulator 302 can be implemented by an electronic component which emits white noise, such as a noisy diode or noisy resistance. The signal is fed to and amplified by amplifier stages (transistors/operational amplifiers), producing a signal which is amplitude-modulated by the noise. The overall interfering signal bandwidth is sufficient to block all control signal channels bandwidth. 2) Digital noise - modulator 302 is implemented as an electronic component which generates pseudo random bits.

An additional method of blocking cellular system operation is to operate jamming device so as to produce a continuous blocking signal on all of the control frequencies of the cellular system. In this method, switch 304 selects the signal frequency comb oscillator 301 output, as a wide bandwidth oscillator, covering all of the control frequency spectrum per cellular standard implementation in said territory.

In another additional method of blocking cellular system operation, jamming device is operated to produce a continuous blocking signal on a selected group of control frequencies. In this case, switch 304 selects the signal frequency comb oscillator 301 output, as a sweep of frequencies. This signal is assembled from multiple predetermined frequencies in simultaneous fashion. A set of frequencies intended for blocking is chosen from all the possible frequencies of the blocked system.

Still another additional method of blocking cellular system operation involves operating jamming device as in the previous methods, with modulator 302 applying modulation to the blocking technique. The blocking signal generated by signal oscillator 30 feeds the input to transmitter 35, which amplifies it and broadcasts it to the atmosphere by antenna 33. Transmitter 35 is based on a linear amplification module operating in the RF range of the cellular frequencies, enabling control of the transmitter power output. The antenna 33 must be matched to the area to be blocked and the location as required. For example, blocking in a single room can be achieved by a printed circuit antenna installed within the jammer device board. In order to achieve accurate coverage, use of sector antennas, phased array antennas or any other means of directional radiation of RF signals known in the art. In the case of a long corridor, the blocking could be achieved by use of a leaky coax cable for the antenna 33, etc. In the previously described embodiments, the set of frequencies intended for blocking is chosen from all the possible frequencies of the system, and these control frequencies are generally known in accordance with the cellular standard.

In another improved embodiment, illustrated in FIG. 4, there is an electronic device 40 featuring an alternative design in accordance with the principles of the present invention, for preventing cellular phone calls in a given regulated area. A reverse control frequency of the mobile unit is detected during a handshake attempt and a

frequency mixing technique is used to generate the matching duplex forward control frequency at which the cellular base station transmits. The generated duplex signal induces open loop oscillations which interfere with the decoding procedure and introduces phase noise. As shown, device 40 comprises a combined receiver/transmitter, with receiver portion 42 comprising an antenna 421, filter 422, pre-amplifier 423, and frequency mixer 424, which is fed with a frequency signal from a local oscillator 425. The pre-amplifier 423 may be configured with a threshold level responsive to a typical reverse control channel transmitted by a mobile unit located within the regulated area. This is to ensure that reverse control channel signals originating outside the regulated area do not trigger any interfering response. The frequency generated by local oscillator 425 is predetermined to be at the exact frequency deviation between the duplex frequencies of the reverse control channel (RCC) and forward control channel (FCC). For example, as per TDMA Standard IS-136, the frequency deviation between RCC and FCC frequencies should be 45.000 MHz. Thus, the output of mixer 424 consists of four different frequencies, one of them being the exact FCC frequency matching the duplex RCC frequency initially received by antenna 421. The mixer 424 output is coupled via a coupler 412 to the transmitter portion 41 of device 40. Transmitter portion 41 comprises a bandpass filter 413 which passes only the FCC frequency to a pre-amplifier 415, via a threshold circuit 414. The output is then fed to a delay and modulation unit 416, after which an amplifier 417 feeds the output to a bandpass filter 418, with its output signal being broadcast via matched antenna 419. The broadcast signal is received by another antenna 411, which is matched to the FCC f. If the loop gain, i.e., the gain applied to the FCC signal received through antenna 411, until it is re-broadcast on antenna 419, is equal to or greater than the isolation between the antennas 411-419, then an unstable oscillation is developed, at the FCC frequency, due to positive feedback. This interferes with decoding and introduces phase noise in the cellular mobile unit, causing the handshake routine to malfunction, thereby disabling cellular system operation.

Using the embodiment of FIG. 4, another method of blocking cellular system operation is by operating local oscillator 425 so as to modulate the received FCC signal with 15 KHz, for example. This causes the broadcast of an amplified,

modulated signal at the same FCC frequency, however, containing a component of phase noise which interferes with decoding in the cellular mobile unit.

Most geographical areas may be covered by several cellular systems. In locations covered by several systems, the control channels transmitted by the different base stations are received by the mobile units at different power levels. A jamming device transmitting at an equal power level on all control frequencies used by cellular systems, without the capability to differentiate between control channels received at different power levels, will result in inaccurate coverage. A cellular system with base station closer to the regulated location may be received at a higher level than control channels received from another base station of a different system. Similarly a base station transmitting at a high power level will be typically received at a higher signal strength, and higher transmission power will be required in order to jam it.

It is therefore important to enable calibration of the output power in a plurality of frequency bands with reference to the signal strength received from base stations transmitting on each band.

The jammer device of FIG. 3 incorporates two channels, each including a separate gain control circuit. Said gain control circuit can be calibrated, either manually by means of trimmer devices, or automatically by means of reference signals responsive to signal strength measurements taken by power sensing devices within and outside the regulated area.

FIG. 3 illustrates two low power signal oscillators 30 and 31, each tuned to a different frequency band, and calibrated to generate a different output power level so as to enable separate coverage to three frequency bands.

It is an objective of the present invention is to provide a reliable method and system for accurate coverage of a given area. In many cases, the isolation between the regulated area and areas surrounding it may be insufficient. Such conditions may also arise due to variations in the output power radiated from cellular base stations nearby the regulated area. In principle a jamming device may be installed and calibrated with reference to the environmental conditions at the time of installation. However, in the event that sometime after installation, a nearby cellular base station increases or decreases its average output power or antenna gain, the jamming signal may become

under or over-powered. A dynamic calibration and control device is configured to sample the environmental control channel signal power, as required - continuously, at regular periodic intervals or each time the jamming device is activated. Such measurements can be taken from several points within or outside the regulated area. A closed loop feedback system may be configured to increase the accuracy of interfering signal coverage. Accordingly, feedback signals from a plurality of measurement points may serve to control the output power and/or radiation pattern of a directional antenna (e.g., phased array).

Referring now to FIG. 7, a jammer unit 74 is installed within regulated area 71 and transmits an interfering signal, which block cellular communications with mobile unit 72 located within the regulated area 71. Sensor device 75 is located outside the regulated area and is tuned to at least one control channel transmitted from a cellular base station. Said sensor comprises receiver and decoder devices having characteristics similar to mobile unit 72. While jammer unit 74 transmits an interfering signal, sensor device 75 performs a decoding function of said control channel and determines whether the interfering signal transmitted by jammer unit 74 blocks cellular communications outside said regulated area 71. Sensor device 75 is connected to jammer unit 74 and transfers a feedback signal responsive to sensor's ability to decode said control channel. Additional sensors similar to sensor device 75 are installed inside the regulated area. Jammer unit 74 uses said feedback signal to transmit an interfering signal with output power and beam which although blocks all cellular communications within regulated area 71, still enables cellular communications outside the regulated area.

In another embodiment a RSSI sensor device is located within the regulated area, jammer unit pauses noise transmission for a short interval (e.g., 3 mSec) and measures the signal strength received from cellular base stations so as to provide a reference for any modifications required for noise transmission output power.

A further improvement over the device of FIG. 3 is the ability to perform real-time screening of incoming and outgoing calls in accordance with a predetermined filtering scheme. Various applications require a blocking device to discriminate between different subscribers. Such is the case in security oriented environments where certain

officers are competent to conduct cellular telephone conversations. The following embodiment enables active bi-directional call screening of all cellular communications taking place within a given area.

FIG. 5 illustrates an electronic calibration and control device 50 that scans control channel frequencies and provides received signal strength indication (RSSI) per each control channel received at a given location. A method for generating RSSI is disclosed in U.S. Patent No. 5,142,695 issued on Aug. 25, 1992 to Roberts et al for "CELLULAR RADIO-TELEPHONE RECEIVER EMPLOYING IMPROVED TECHNIQUE FOR GENERATING AN INDICATION OF RECEIVED SIGNAL STRENGTH", which is incorporated by reference herein. It should be understood that the present invention is not limited to any particular RSSI measurement technique. Device 50 recovers a digital control channel from a digitally encoded, quadrature-modulated RF signal received at antenna 501. The front-end mixer 502 mixes the received signal with a locally generated signal from a frequency synthesizer 503 for tuning to a plurality of control channels within a predefined frequency range, as set out in the cellular standard involved. The output of the front-end mixer 502 is a signal having a selected frequency spectrum centered on a selected intermediate frequency. The frequency of the locally generated signal is determined by a control signal sent from the CPU 516 to the receive synthesizer 503. The VGA 504 amplifies the output of the front-end mixer 502 with a gain controlled by a VGA control signal received from MUX 515. A demodulation and signal processing circuit 52 is preceded by a frequency converting circuit 51 having a local oscillator 505 and a pair of mixers 506-507. Each of the mixers 506-507 combines the amplified signal from the VGA 504 with one of two orthogonally related baseband signals generated by local oscillator 505. The analog baseband signals are applied to separate "I" and "Q" circuit paths for conversion into digital baseband signals by A/D converters 508-509 and processing by DSPs 510-511, respectively. The DSPs 510-511 perform baseband match filter functions and demodulate the digital signals from the A/D converters 508-509, thereby generating demodulated digital baseband signals. The decoder 512 recovers the data by reversing the signal encoding algorithm used by the base station (e.g., QPSK). The recovered control channel data is transferred to the CPU 516. The demodulated digital baseband signals from DSPs 510-511 are also fed into automatic gain control circuit (AGC) 513, combined and converted into an AGC signal

responsive to the amplitudes of the signal envelope, and therefore the received signal. The ramp generator 514 generates a ramp signal, i.e., a signal having a generally increasing amplitude over a preselected period of time (e.g., a digital counter). In response to a select signal SEL from CPU 516, digital multiplexer (MUX) 515 passes either AGC signal or the ramp signal to the VGA 504 as the VGA control signal. The CPU 516 also controls the start and termination of the ramp signal by means of a timing signal SYNC applied to the ramp generator 514. In addition to providing the control signal to the VGA 504, the MUX 515 applies the control signal to the look-up table memory 517, which stores a plurality of potential RSSI values, each corresponding to a VGA control value. CPU 516 stores a list of control channel frequencies, each with its measured signal strength in memory device 518.

In order to cope with several control channel frequencies, each having a different signal strength, a frequency hopping transmitter is configured to scan all control channel frequencies detected by device 50 and transmit an interfering signal according to its RSSI value.

FIG. 6 illustrates a frequency hopping transmitter device 60 that is controlled by microprocessor (CPU) device 61 having memory device 62. It should be understood that CPU 61 and memory device 62 can be common to those implemented in device 50 (see FIG. 5 devices 516, 518). The transmitting frequency synthesizer 63 generates the transmitter carrier frequency in accordance with commands from the CPU 61. To implement frequency hopping, the CPU 61 reads hopping information stored in memory device 62 and then sends timed instructions to the transmitter frequency synthesizer 63 to generate a sequence of carrier frequencies in accordance with a frequency hopping scheme based on the set of control channel frequencies and levels detected and measured by device 50, or any similar measurement facility, and recorded in memory device 62. A noise signal from noise source 63 is connected to RF modulator 64, which modulates the carrier frequency from the transmitting frequency synthesizer 63 according to the modulation method most suitable for blocking a particular cellular standard. For example, one suitable modulation for TDMA cellular systems based on EIA/TIA IS-54 is quadrature phase shift keying (QPSK). The power amplifier 66 amplifies the signals from RF modulator 64. The RF power emission level is selected on command by the CPU 61 via D/A converter 67 in

accordance with RSSI levels measured for each control channel and recorded in memory device 62. When used in conjunction with device 50, the output power of transmitter unit 60 is considerably lower than a wide band jamming device such as the device illustrated in FIG. 3. This is especially significant in cellular systems such as GSM or D-AMPS (TDMA) IS-136, where control channel frequencies may be located over a wide frequency range.

In another improved embodiment, one control channel frequency is temporarily removed from the frequency hopping scheme stored in memory device 62 . Device 50 is tuned to decode reverse control channel messages transmitted by all mobile units located within a given regulated area over the duplex channel of the control channel removed. Memory device 62 holds a database of authorized mobile subscribers, for whom call establishment is allowed. Whenever a control channel message indicating call establishment handshake is decoded for unauthorized subscribers, said forward control channel frequency is re-added to the hopping scheme for a period of time sufficient to prevent the handshake between the unauthorized subscriber and the cellular base station. Thereafter, said control channel is removed from the hop-set so as to enable authorized subscribers to communicate with the cellular system over said control channel.

In yet another embodiment, the noise source 64 is replaced with a signaling generator controlled by CPU 61. The latter instructs the signaling generator to transmit phantom base station signaling causing mobile units within a given regulated area to function as if they are registered with a local base station. The base station signaling transmission causes mobile phones to refrain from seeking other control channels. Base station signaling is intentionally controlled not correspond to mobile identification numbers (MIN) which have been defined in the memory device 62 as authorized to conduct communications within the regulated area. Said authorized portable units are rejected by the clone base station, and do not receive base station signaling required in order to complete registration with the clone base station. Thus said authorirzed portable units seek other control channels on which registration can be completed. Since control channels are not affected by said phantom signaling, authorized users can freely communicate with any other available cellular base station in the vicinity of the regulated area.

A significant drawback of the embodiments disclosed herein, which are based on transmission of a continuous (CW) noise signal, is the increase of noise outside the regulated area during operation that might degrade the overall performance of the cellular network by interfering with weak signals transmitted by distant base stations. Furthermore, as various handsets have different receiver sensitivity figures, within specified limits, in extreme conditions, such as those imposed by noise jamming, some subscribers might be influenced by the interference more than others. Moreover, as modern life habits involve increasing exposure to various radiation sources more and more individuals express their concern and prefer not to subject themselves to unnecessary continuous radiation. Accordingly, the following embodiment does not radiate any interfering signal as long as the mobile units within the regulated area are in stand-by mode. Interfering transmission is applied only during the handshake process associated with call establishment.

Referring now to FIG. 8, a jamming device 80 consists of control unit 81, controlled noise transmitter 82, receiver 83, time switch 84 and antenna 85. Receiver 83 includes a RF power detector which is configured to sense RF radiation emitted from mobile units on the reverse control/voice channel frequency band. When a signal is detected by receiver 83 at a minimum predetermined power level, control unit 81 commands the controlled noise transmitter 82 to respond with a noise transmission over the entire bandwidth transmitted from the base station, or any relevant part thereof, for a predetermined period of time. A time switch 84 enables both transmitter 82 and receiver 83 to use the same antenna for transmission and reception as determined by control unit 81. The control unit 81 typically comprises a microprocessor and memory device. The control unit 81 implements the logic by which noise transmission is activated. The controller is configured with various parameters for customizing the jamming device 80 for a given operation environment. In a typical implementation, control unit 81 has a plurality of received frequency bands covered by receiver 83. For each detected transmission in one of said frequency bands, the control unit 81 commands the noise transmitter 82 to generate a responsive interfering signal on the matching channel transmitted by the base station.

For example if the receiver 83 detects a transmission from an AMPS standard mobile unit, handshake between the mobile unit and the base station is prevented by transmission of a RF signal at the duplex transmit frequency , or by jamming the

entire transmit frequency range as expected in a AMPS system, according to AMPS standards. Similarly, when the receiver 83 detects a RF transmission from a TDMA mobile unit, the device transmits a signal on the base station transmit frequency expected in a TDMA system.

It should be understood that when responding over a wide band, more output power is required. However, the tradeoff of responding over a narrow band involves more processing power required for detection of the exact frequency where the interfering signal is likely to have the desired effect over the communications between the mobile unit and the base station.

The controlled noise transmitter 82 may also be calibrated to respond to the RF signal detected with a jamming signal on the entire control and voice communication bandwidth, thereby disabling communications even if the call has already been established.

In an improved embodiment a decoding device monitors the identification signals transmitted by the mobile unit (e.g. MIN / ESN) and compares them with a database held in a memory device prior to initiation of the noise signal transmission by the controlled noise transmitter 82. Thus the device 80 is capable of selectively disabling and enabling communications with predetermined telephone subscribers, effectively providing a cellular communication firewall.

In a CDMA cellular telephone system such as is described in U.S. Pat. No. 4,901,307, issued Feb. 13, 1990, entitled "SPREAD SPECTRUM MULTIPLE ACCESS COMMUNICATION SYSTEM USING SATELLITE OR TERRESTRIAL REPEATERS", assigned to Qualcomm Inc., channel specific pseudonoise (PN) sequences are used instead of frequencies, such as in FDMA or frequency + time-slot as in TDMA. In order to interfere with base station transmitted paging and/or control channels, a jamming device is configured to transmit noise signals modulated and spread by PN sequences used by the cellular system in a given area.

Having described the invention with regard to certain specific embodiments, it is to be understood that the description is not meant as a limitation, since further

modifications may now become apparent to those skilled in the art, and it is intended to cover such modifications as fall within the scope of the appended claims.

We claim:

1. A method for regulation of cellular communications in a communication system within a given area, said method comprising the steps of:

defining at least one frequency existing within the area for conducting cellular communications, said frequency containing information transmitted thereon; and

generating a signal which interferes with said control frequency by preventing decoding of said signals and commands, to prevent cellular communication within the given area.

2. The method of claim 1 wherein said frequency is a forward control channel (FCC) providing communications from the cellular communication system to a portable cellular telephone.

3. The method of claim 1 wherein said frequency is a reverse control channel (RCC) providing communications from a portable cellular telephone to the cellular communication system.

4. The method of claim 1 wherein said at least one frequency comprises a single frequency.

5. The method of claim 1 wherein said frequency comprises a range of relevant control frequencies.

6. The method of claim 1 wherein said frequency is a set of control frequencies selected from a range of relevant control frequencies.

7. The method of claim 1 wherein said interference signal is generated with analog noise.

8. The method of claim 1 wherein said interference signal is generated with digital noise.

9. The method of claim 1 wherein said interference signal is generated continuously on a selected set of control frequencies.

10. The method of claim 1 wherein said interfering signal is transmitted subsequent to transmission originating from portable cellular telephones

11. The method of claim 1 wherein said definition step is performed during a handshake protocol between a cellular communication system and a portable cellular telephone, and wherein said generating step is performed by modulating said defined frequency with a frequency representing the deviation between duplex forward and reverse frequencies, and interferes with cellular communication by introducing phase noise in said portable cellular telephone.

12. The method of claim 1 wherein said definition step is performed during a handshake between a cellular communication system and a portable cellular telephone, and wherein said generating step is performed by modulating said defined frequency with a predetermined frequency to develop a phase modulated signal, which blocks decoding of a forward control channel signal by introducing phase noise in said portable cellular telephone.

13. The method of claim 1 wherein said interfering signal transmission power is a function of signal strength of signal received from the base station within said area.

14. The method of claim 1 wherein said interfering signal transmission power is a function of signal strength of signal received from the base station within and outside said area.

15. The method of claim 1 wherein said interfering signal is transmitted only subsequent to transmissions originating from portable cellular telephones which have not been authorized for cellular communication within said area.

16. The method of claim1 wherein said interfering signal is transmitted on a plurality of frequencies at a plurality of power levels respective to each cellular system characteristics.

17. The method of claim1 wherein said interfering signal is transmitted at different power levels respective to cellular standards and signal strength of signal received from the base station within said area.

18. The method of claim1 wherein said interfering signal is generated from within said regulated area.

19. The method of claim1 wherein said interfering signal is generated from outside said regulated area.

20. A device for regulation of cellular telephone calls in a communication system within a given area, said device comprising: means for defining at least one control frequency existing within the area for establishing cellular telephone calls, and means for generating a signal which interferes with said control frequency by preventing decoding of said signals and commands.

21. The device of claim 20 wherein said control frequency is a forward control channel (FCC) providing communications from the cellular communication system to a portable cellular telephone.

22. The device of claim 20 wherein said control frequency is a reverse control channel (RCC) providing communications from a portable cellular telephone to the cellular communication system.

23. The device of claim 20 wherein said at least one control frequency comprises a single frequency.

24. The device of claim 20 wherein said control frequency comprises a range of relevant control frequencies.

25. The device of claim 20 wherein said control frequency is a set of control frequencies selected from a range of relevant control frequencies.

26. The device of claim 20 wherein said means for generating comprises a mixer for mixing said determined control frequency with a frequency representing the deviation between duplex forward and reverse control channel frequencies, thereby developing an unstable positive feedback oscillation in one of said control channel frequencies, and blocking decoding by introducing phase noise in said portable cellular telephone.

27. The device of claim 20 wherein said means for generating comprises a mixer for mixing said determined control frequency with a predetermined frequency to develop a phase modulated signal, which blocks decoding of a forward control channel signal by introducing phase noise in said portable cellular telephone.

28. A method for regulating cellular communications between a plurality of cellular base stations and a plurality of mobile units located within a given regulated area comprising the steps of:
defining at least one frequency band used for transmission by mobile units; and
receiving signals transmitted by said mobile units; and
responding with a response transmission on the frequency band used for transmission by said cellular base stations for a predetermined duration.

29. The method of claim 28, wherein said response transmission characteristics are respective to said received signal characteristics.

30. The method of claim 28, wherein said response transmission is noise generated over the entire frequency band allocated for base station transmission.

31. The method of claim 28, wherein said response transmission is noise generated over a narrow frequency band determined in accordance with said received signal .

32. The method of claim 28, wherein said response transmission is generated for a duration respective to said received signal.

33. The method of claim 28, wherein said response transmission is generated at a transmission power respective to said received signal.

34. The method of claim 28, wherein said response transmission includes base station signaling respective to said received signal.

35. A method for regulation of cellular communications in a communication system within a given area, said method comprising the steps of: transmitting phantom base station signaling on a cellular standard control channel, said signaling causing mobile units within a given regulated area to refrain from registration with a other local base stations thus disabling communications with the cellular network from within said area.

36. The method of claim 35, wherein said phantom base station signaling is not respective to enabled telephones, thus enabling subscribers which have been defined as authorized for cellular communications within said area to register with a real local base station and conduct communications.

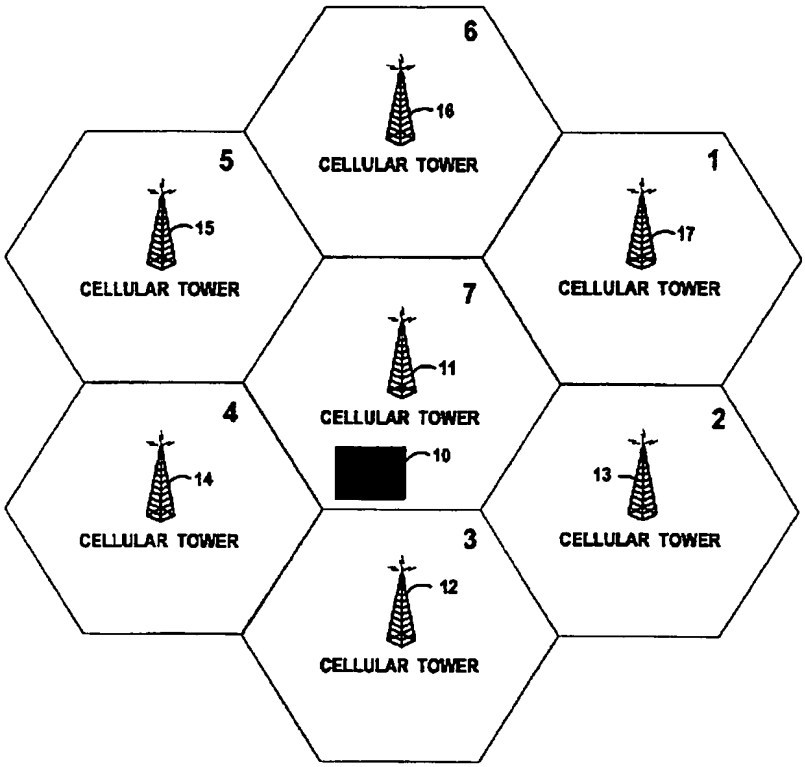

6
16
CELLULAR TOWER
5
15
CELLULAR TOWER
1
17
CELLULAR TOWER
7
11
CELLULAR TOWER
10
4
14
CELLULAR TOWER
2
13
CELLULAR TOWER
3
12
CELLULAR TOWER

FIG. 1

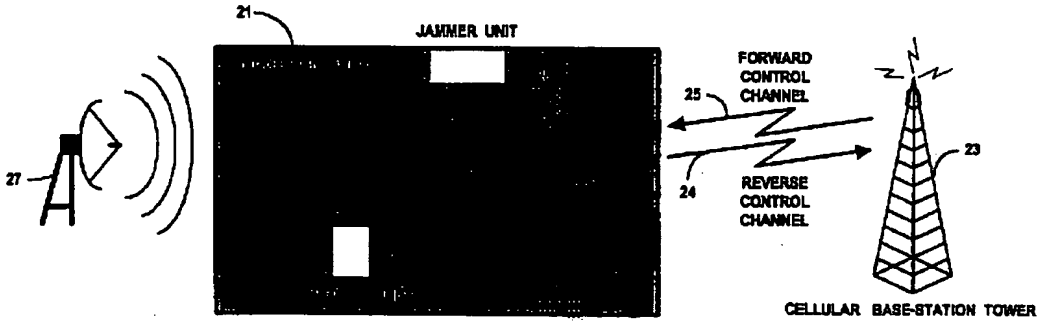

21
JAMMER UNIT
27
FORWARD CONTROL CHANNEL
25
24
REVERSE CONTROL CHANNEL
23
CELLULAR BASE-STATION TOWER

FIG. 2

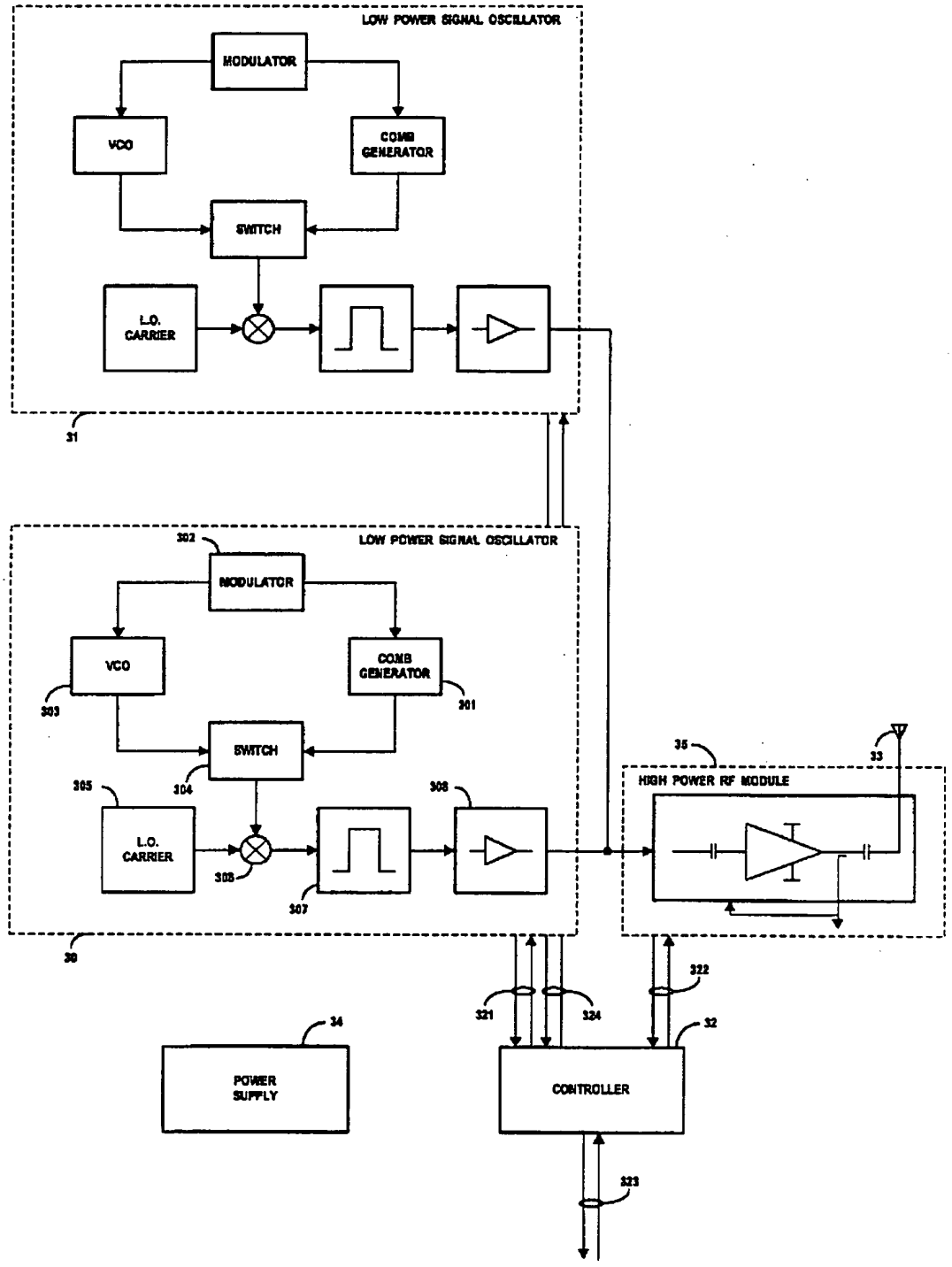

LOW POWER SIGNAL OSCILLATOR
MODULATOR
VCO
COMB GENERATOR
SWITCH
L.O. CARRIER
31
LOW POWER SIGNAL OSCILLATOR
302
MODULATOR
VCO
303
COMB GENERATOR
301
SWITCH
304
305
L.O. CARRIER
306
307
308
30
35
33
HIGH POWER RF MODULE
322
321
324
34
POWER SUPPLY
32
CONTROLLER
323

FIG. 3

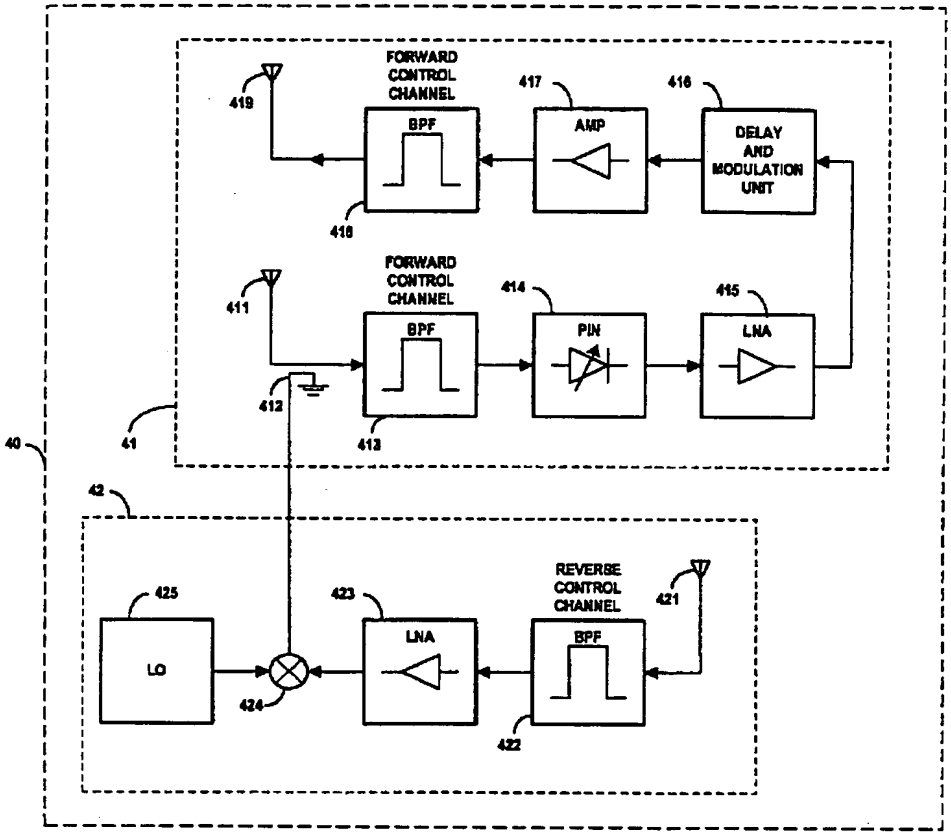

FORWARD CONTROL CHANNEL
BPF
AMP
DELAY AND MODULATION UNIT
FORWARD CONTROL CHANNEL
BPF
PIN
LNA
REVERSE CONTROL CHANNEL
BPF
LNA
LO
40
41
42
411
412
413
414
415
416
417
418
419
421
422
423
424
425

FIG. 4

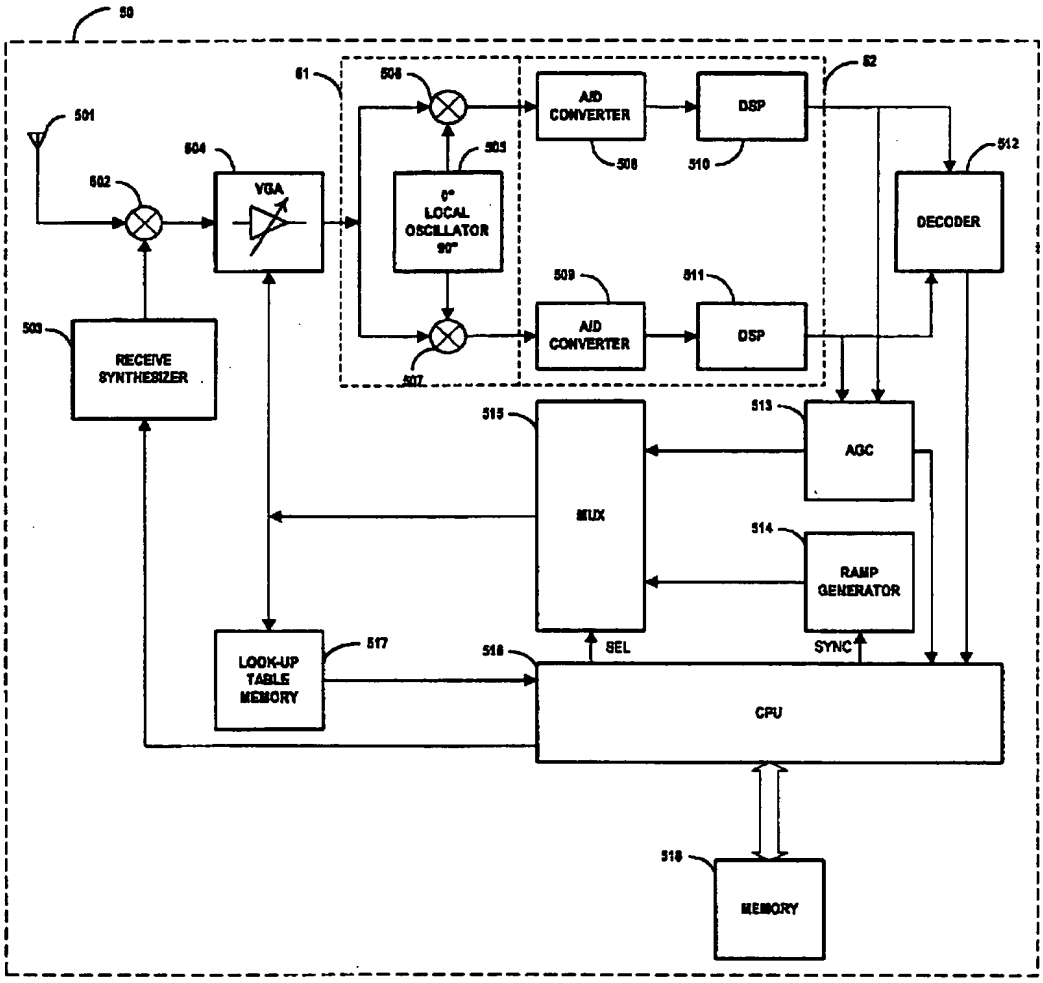

50
61
501
502
504
VGA
505
0°
LOCAL
OSCILLATOR
90°
506
A/D
CONVERTER
508
DSP
510
62
512
DECODER
503
RECEIVE
SYNTHESIZER
507
509
A/D
CONVERTER
511
DSP
515
MUX
513
AGC
514
RAMP
GENERATOR
SEL
SYNC
517
LOOK-UP
TABLE
MEMORY
516
CPU
518
MEMORY

FIG. 5

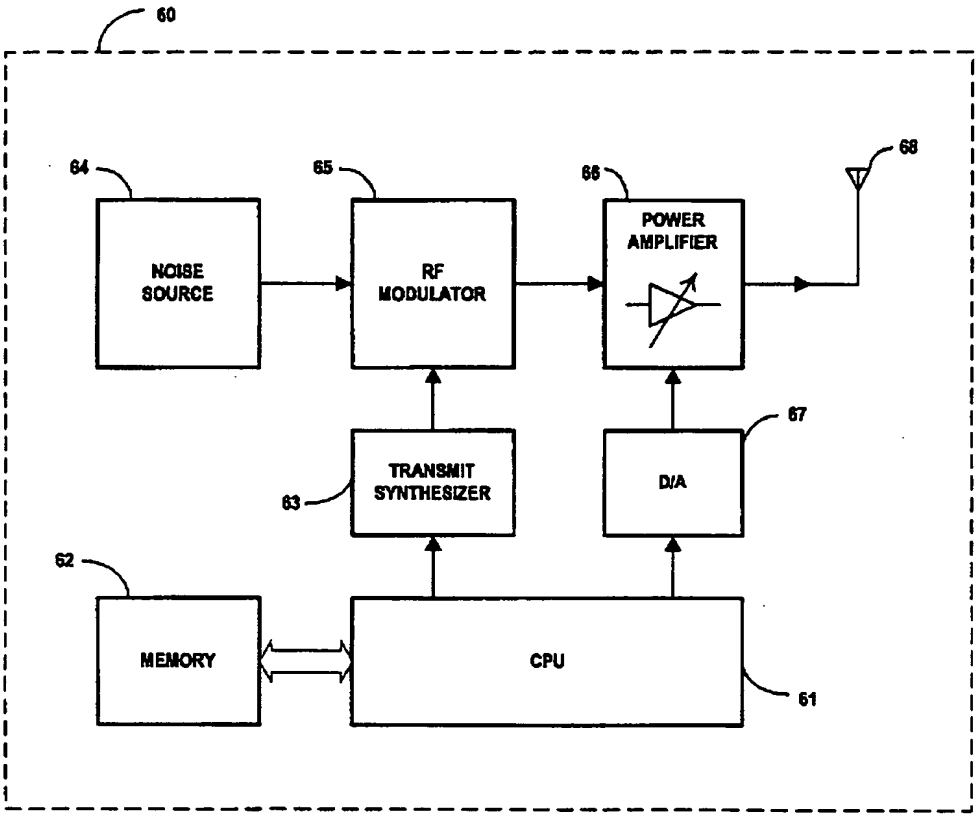

60
64
NOISE SOURCE
65
RF MODULATOR
66
POWER AMPLIFIER
68
63
TRANSMIT SYNTHESIZER
67
D/A
62
MEMORY
CPU
61

FIG. 6

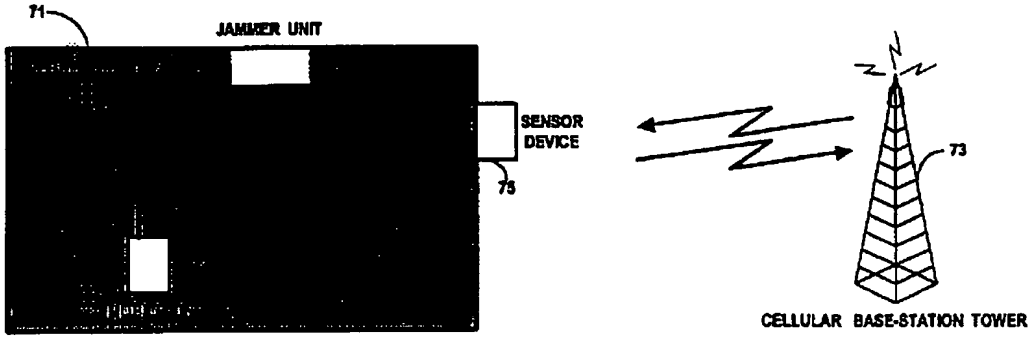

71
JAMMER UNIT
SENSOR DEVICE
75
73
CELLULAR BASE-STATION TOWER

FIG. 7

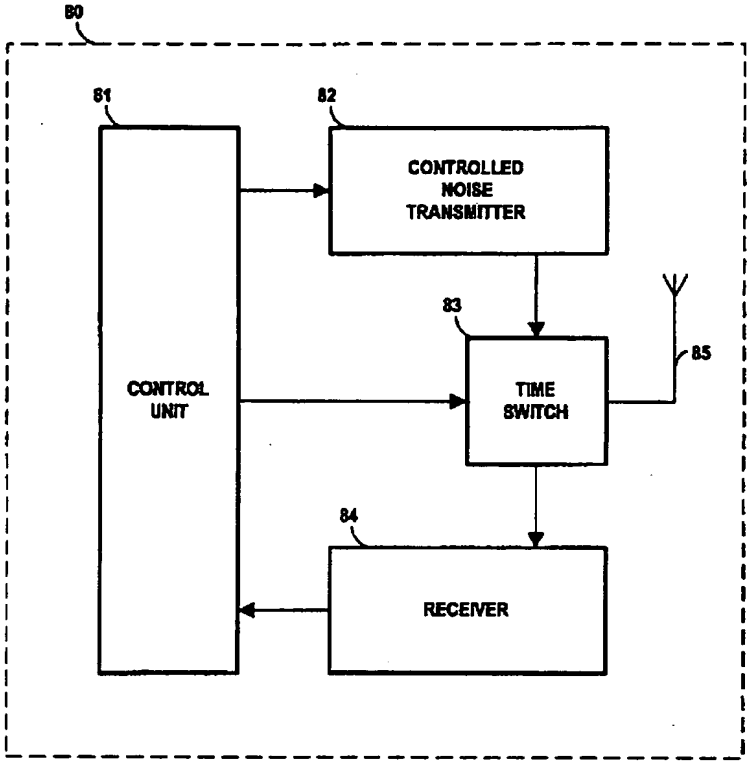

80
81
82
CONTROLLED NOISE TRANSMITTER
83
85
CONTROL UNIT
TIME SWITCH
84
RECEIVER

FIG. 8